目次

概要
主な問題
シナリオ
使用したデバッグ
IOS ルータの設定
暗号化設定
相手側
デバッグ
IOS 応答側
メイン モード メッセージ 1（MM1）
メイン モード メッセージ 2（MM2）：応答の送信
メイン モード メッセージ 3（MM3）
メイン モード メッセージ 4（MM4）
メイン モード メッセージ 5（MM5）：発信側が ID を送信します。
メイン モード メッセージ 6（MM6）：発信側が ID を送信します。 フェーズ 1 が完了します。
クイック モード メッセージ 1（QM1）
クイック モード メッセージ 2（QM2）
クイック モード メッセージ 3（QM3）：フェーズ 2 が完了し、トンネル インターフェイスがアップします。
IOS ルータ：発信側
メイン モード メッセージ 1（MM1）：初期のやり取り
メイン モード メッセージ 2（MM2）：初期のやり取りへの応答
メイン モード メッセージ 3（MM3）：NAT 検出および Diffie-Hellman 交換
メイン モード メッセージ 4（MM4）：NAT 検出および Diffie-Hellman 交換
メイン モード メッセージ 5（MM5）：ID の送信
メイン モード メッセージ 6（MM6）：リモート ピア ID、フェーズ 1 が確立されます。
クイック モード メッセージ 1（QM1）：ピアがフェーズ 2 を開始します。
クイック モード メッセージ 2（QM2）
クイック モード メッセージ 3（QM3）：フェーズ 2 の確立
トンネルの確認
関連情報

概要

このドキュメントには、メイン モードと事前共有キー（PSK）を使用する際の Cisco IOS® ソフトウェアでのデバッグを理解するための情報が記載されています。

また、特定のデバッグ行を設定に変換する方法に関する情報を提供します。

次のトピックについては取り上げません。

- トンネルが確立した後の通過トラフィック
- IPSec またはインターネット キー交換（IKE）の基本概念

主な問題

IKE および IPSec のデバッグはわかりにくくなりがちです。 通常、Cisco Technical Assistance Center（TAC）はこれらのデバッグを使用して、IPSec VPN トンネル**確立**の問題が発生している場所を特定します。

シナリオ

メイン モードは通常、LAN-to-LAN トンネル間に使用されるか、リモート アクセス（ezvpn）の場合は認証に証明書を使用するときに使用されます。

これらのデバッグは、15.2(1)T ソフトウェア リリースを実行する Cisco IOS デバイスから行われます。

このドキュメントでは、次の 2 つの主なシナリオについて説明します。

- IOS 発信側
- IOS 応答側

このドキュメントでは、2 つのサイト間の VTI ベースのトンネルが IPv6 に基づいて確立されます。

> **注**：
>
> このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用します。
>
> debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

使用したデバッグ

- debug crypto isakmp
- debug crypto ipsec
- debug crypto kmi

IOS ルータの設定

暗号化設定

相手側

デバッグ

IOS 応答側

メイン モード メッセージ 1 (MM1)

IKE の初期提案には次が含まれます。

- 暗号化
- ハッシュ
- Diffie-Hellman (DH) グループ
- ライフタイム

関連する設定：

メイン モード メッセージ 2 (MM2) : 応答の送信

メイン モード メッセージ 3 (MM3)

次が含まれます。

- ネットワーク アドレス変換 (NAT) 検出
- DH 交換部分 1

メイン モード メッセージ 4 (MM4)

次が含まれます。

- NAT 検出ペイロード
- DH 交換の続き

メイン モード メッセージ 5 (MM5) : 発信側が ID を送信します。

次が含まれます。

- ローカル ID 情報
- キー

メイン モード メッセージ 6 (MM6) : 応答側が ID を送信します。 フェーズ 1 が完了します。

次が含まれます。

- ピアから送信されたリモート ID
- 選択するトンネル グループに関する最終決定

関連する設定：

クイック モード メッセージ 1 (QM1)

```
*Sep 21 08:33:43.433: ISAKMP (1011): received packet from 2001: DB8::2 dport
500 sport 500 Global (R) QM_IDLE
*Sep 21 08:33:43.433: ISAKMP: set new node 1371333358 to QM_IDLE
*Sep 21 08:33:43.433: ISAKMP: (1011): processing HASH payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011): processing SA payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011):Checking IPSec proposal 1
*Sep 21 08:33:43.433: ISAKMP: transform 1, ESP_AES
*Sep 21 08:33:43.433: ISAKMP:   attributes in transform:
*Sep 21 08:33:43.433: ISAKMP:      encaps is 1 (Tunnel)
*Sep 21 08:33:43.433: ISAKMP:      SA life type in seconds
*Sep 21 08:33:43.433: ISAKMP:      SA life duration (basic) of 3600
*Sep 21 08:33:43.433: ISAKMP:      SA life type in kilobytes
*Sep 21 08:33:43.433: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
*Sep 21 08:33:43.433: ISAKMP:      authenticator is HMAC-SHA
*Sep 21 08:33:43.433: ISAKMP:      key length is 128
*Sep 21 08:33:43.433: ISAKMP: (1011):atts are acceptable.
*Sep 21 08:33:43.433: IPSEC(validate_proposal_request): proposal part #1
*Sep 21 08:33:43.433: IPSEC(validate_proposal_request): proposal part #1,
 (key eng. msg.) INBOUND local= 2001: DB8::3:0, remote= 2001: DB8::2:0,
    local_proxy= ::/0/256/0,
    remote_proxy= ::/0/256/0,
   protocol= ESP, transform= NONE  (Tunnel),
   lifedur= 0s and 0kb,
   spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0
*Sep 21 08:33:43.433: ISAKMP: (1011): processing NONCE payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011): processing ID payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011): processing ID payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011):QM Responder gets spi
*Sep 21 08:33:43.433: ISAKMP: (1011):Node 1371333358, Input =
IKE_MESG_FROM_PEER, IKE_QM_EXCH
*Sep 21 08:33:43.433: ISAKMP: (1011): Old State = IKE_QM_READY  New State =
IKE_QM_SPI_STARVE
```

関連コンフィギュレーション：

```
*Sep 21 08:33:43.433: ISAKMP (1011): received packet from 2001: DB8::2 dport
500 sport 500 Global (R) QM_IDLE
*Sep 21 08:33:43.433: ISAKMP: set new node 1371333358 to QM_IDLE
*Sep 21 08:33:43.433: ISAKMP: (1011): processing HASH payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011): processing SA payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011):Checking IPSec proposal 1
*Sep 21 08:33:43.433: ISAKMP: transform 1, ESP_AES
*Sep 21 08:33:43.433: ISAKMP:   attributes in transform:
*Sep 21 08:33:43.433: ISAKMP:      encaps is 1 (Tunnel)
*Sep 21 08:33:43.433: ISAKMP:      SA life type in seconds
*Sep 21 08:33:43.433: ISAKMP:      SA life duration (basic) of 3600
*Sep 21 08:33:43.433: ISAKMP:      SA life type in kilobytes
*Sep 21 08:33:43.433: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
*Sep 21 08:33:43.433: ISAKMP:      authenticator is HMAC-SHA
*Sep 21 08:33:43.433: ISAKMP:      key length is 128
*Sep 21 08:33:43.433: ISAKMP: (1011):atts are acceptable.
```

```
*Sep 21 08:33:43.433: IPSEC(validate_proposal_request): proposal part #1
*Sep 21 08:33:43.433: IPSEC(validate_proposal_request): proposal part #1,
 (key eng. msg.) INBOUND local= 2001: DB8::3:0, remote= 2001: DB8::2:0,
    local_proxy= ::/0/256/0,
    remote_proxy= ::/0/256/0,
   protocol= ESP, transform= NONE  (Tunnel),
   lifedur= 0s and 0kb,
   spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0
*Sep 21 08:33:43.433: ISAKMP: (1011): processing NONCE payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011): processing ID payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011): processing ID payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011):QM Responder gets spi
*Sep 21 08:33:43.433: ISAKMP: (1011):Node 1371333358, Input =
IKE_MESG_FROM_PEER, IKE_QM_EXCH
*Sep 21 08:33:43.433: ISAKMP: (1011): Old State = IKE_QM_READY  New State =
IKE_QM_SPI_STARVE
```

クイック モード メッセージ 2 (QM2)

次が含まれます。

- リモート エンドがパラメータを送信します。
- 提案された 2 つのフェーズ 2 ライフタイムのうち短い方が選択されます。

```
*Sep 21 08:33:43.433: ISAKMP (1011): received packet from 2001: DB8::2 dport
500 sport 500 Global (R) QM_IDLE
*Sep 21 08:33:43.433: ISAKMP: set new node 1371333358 to QM_IDLE
*Sep 21 08:33:43.433: ISAKMP: (1011): processing HASH payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011): processing SA payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011):Checking IPSec proposal 1
*Sep 21 08:33:43.433: ISAKMP: transform 1, ESP_AES
*Sep 21 08:33:43.433: ISAKMP:   attributes in transform:
*Sep 21 08:33:43.433: ISAKMP:      encaps is 1 (Tunnel)
*Sep 21 08:33:43.433: ISAKMP:      SA life type in seconds
*Sep 21 08:33:43.433: ISAKMP:      SA life duration (basic) of 3600
*Sep 21 08:33:43.433: ISAKMP:      SA life type in kilobytes
*Sep 21 08:33:43.433: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
*Sep 21 08:33:43.433: ISAKMP:      authenticator is HMAC-SHA
*Sep 21 08:33:43.433: ISAKMP:      key length is 128
*Sep 21 08:33:43.433: ISAKMP: (1011):atts are acceptable.
*Sep 21 08:33:43.433: IPSEC(validate_proposal_request): proposal part #1
*Sep 21 08:33:43.433: IPSEC(validate_proposal_request): proposal part #1,
 (key eng. msg.) INBOUND local= 2001: DB8::3:0, remote= 2001: DB8::2:0,
    local_proxy= ::/0/256/0,
    remote_proxy= ::/0/256/0,
   protocol= ESP, transform= NONE  (Tunnel),
   lifedur= 0s and 0kb,
   spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0
*Sep 21 08:33:43.433: ISAKMP: (1011): processing NONCE payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011): processing ID payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011): processing ID payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011):QM Responder gets spi
*Sep 21 08:33:43.433: ISAKMP: (1011):Node 1371333358, Input =
```

```
IKE_MESG_FROM_PEER, IKE_QM_EXCH
*Sep 21 08:33:43.433: ISAKMP: (1011): Old State = IKE_QM_READY  New State =
IKE_QM_SPI_STARVE
```

関連コンフィギュレーション：

```
*Sep 21 08:33:43.433: ISAKMP (1011): received packet from 2001: DB8::2 dport
500 sport 500 Global (R) QM_IDLE
*Sep 21 08:33:43.433: ISAKMP: set new node 1371333358 to QM_IDLE
*Sep 21 08:33:43.433: ISAKMP: (1011): processing HASH payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011): processing SA payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011):Checking IPSec proposal 1
*Sep 21 08:33:43.433: ISAKMP: transform 1, ESP_AES
*Sep 21 08:33:43.433: ISAKMP:   attributes in transform:
*Sep 21 08:33:43.433: ISAKMP:      encaps is 1 (Tunnel)
*Sep 21 08:33:43.433: ISAKMP:      SA life type in seconds
*Sep 21 08:33:43.433: ISAKMP:      SA life duration (basic) of 3600
*Sep 21 08:33:43.433: ISAKMP:      SA life type in kilobytes
*Sep 21 08:33:43.433: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
*Sep 21 08:33:43.433: ISAKMP:      authenticator is HMAC-SHA
*Sep 21 08:33:43.433: ISAKMP:      key length is 128
*Sep 21 08:33:43.433: ISAKMP: (1011):atts are acceptable.
*Sep 21 08:33:43.433: IPSEC(validate_proposal_request): proposal part #1
*Sep 21 08:33:43.433: IPSEC(validate_proposal_request): proposal part #1,
 (key eng. msg.) INBOUND local= 2001: DB8::3:0, remote= 2001: DB8::2:0,
    local_proxy= ::/0/256/0,
    remote_proxy= ::/0/256/0,
   protocol= ESP, transform= NONE  (Tunnel),
   lifedur= 0s and 0kb,
   spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0
*Sep 21 08:33:43.433: ISAKMP: (1011): processing NONCE payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011): processing ID payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011): processing ID payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011):QM Responder gets spi
*Sep 21 08:33:43.433: ISAKMP: (1011):Node 1371333358, Input =
IKE_MESG_FROM_PEER, IKE_QM_EXCH
*Sep 21 08:33:43.433: ISAKMP: (1011): Old State = IKE_QM_READY  New State =
IKE_QM_SPI_STARVE
```

クイック モード メッセージ 3（QM3）：フェーズ 2 が完了し、トンネル インターフェイスがアップします。

```
*Sep 21 08:33:43.437: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel23,
changed state to up
*Sep 21 08:33:43.437: ISAKMP (1011): received packet from 2001: DB8::2 dport
500 sport 500 Global (R) QM_IDLE
*Sep 21 08:33:43.437: ISAKMP: (1011): deleting node 1371333358 error FALSE
reason "QM done (await)"
*Sep 21 08:33:43.437: ISAKMP: (1011):Node 1371333358, Input =
IKE_MESG_FROM_PEER, IKE_QM_EXCH
*Sep 21 08:33:43.437: ISAKMP: (1011): Old State = IKE_QM_R_QM2  New State =
IKE_QM_PHASE2_COMPLETE
*Sep 21 08:33:43.437: IPSEC(key_engine): got a queue event with 1 KMI message(s
*Sep 21 08:33:43.437: IPSEC(key_engine_enable_outbound): rec'd enable notify
from ISAKMP
```

IOS ルータ：発信側

メイン モード メッセージ 1（MM1）：初期のやり取り

次が含まれます。

- ベンダー ID（VID）
- 容量
- フェーズ 1 の提案
- IKE セキュリティ アソシエーション（SA）
- IPSec はすでに SA のテンプレートを作成します。

```
*Sep 21 08:33:43.437: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel23,
changed state to up
*Sep 21 08:33:43.437: ISAKMP (1011): received packet from 2001: DB8::2 dport
500 sport 500 Global (R) QM_IDLE
*Sep 21 08:33:43.437: ISAKMP: (1011): deleting node 1371333358 error FALSE
reason "QM done (await)"
*Sep 21 08:33:43.437: ISAKMP: (1011):Node 1371333358, Input =
IKE_MESG_FROM_PEER, IKE_QM_EXCH
*Sep 21 08:33:43.437: ISAKMP: (1011): Old State = IKE_QM_R_QM2  New State =
IKE_QM_PHASE2_COMPLETE
*Sep 21 08:33:43.437: IPSEC(key_engine): got a queue event with 1 KMI message(s
*Sep 21 08:33:43.437: IPSEC(key_engine_enable_outbound): rec'd enable notify
from ISAKMP
```

関連コンフィギュレーション：

```
*Sep 21 08:33:43.437: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel23,
changed state to up
*Sep 21 08:33:43.437: ISAKMP (1011): received packet from 2001: DB8::2 dport
500 sport 500 Global (R) QM_IDLE
*Sep 21 08:33:43.437: ISAKMP: (1011): deleting node 1371333358 error FALSE
reason "QM done (await)"
*Sep 21 08:33:43.437: ISAKMP: (1011):Node 1371333358, Input =
IKE_MESG_FROM_PEER, IKE_QM_EXCH
*Sep 21 08:33:43.437: ISAKMP: (1011): Old State = IKE_QM_R_QM2  New State =
IKE_QM_PHASE2_COMPLETE
*Sep 21 08:33:43.437: IPSEC(key_engine): got a queue event with 1 KMI message(s
*Sep 21 08:33:43.437: IPSEC(key_engine_enable_outbound): rec'd enable notify
from ISAKMP
```

メイン モード メッセージ 2（MM2）：初期のやり取りへの応答

次が含まれます。

- ピアが、使用する Internet Security Association and Key Management Protocol（ISAKMP）ポリシーを選択します。
- IKE SA

```
*Sep 21 08:33:43.437: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel23,
changed state to up
*Sep 21 08:33:43.437: ISAKMP (1011): received packet from 2001: DB8::2 dport
500 sport 500 Global (R) QM_IDLE
*Sep 21 08:33:43.437: ISAKMP: (1011): deleting node 1371333358 error FALSE
reason "QM done (await)"
*Sep 21 08:33:43.437: ISAKMP: (1011):Node 1371333358, Input =
IKE_MESG_FROM_PEER, IKE_QM_EXCH
*Sep 21 08:33:43.437: ISAKMP: (1011): Old State = IKE_QM_R_QM2  New State =
IKE_QM_PHASE2_COMPLETE
```

```
*Sep 21 08:33:43.437: IPSEC(key_engine): got a queue event with 1 KMI message(s
*Sep 21 08:33:43.437: IPSEC(key_engine_enable_outbound): rec'd enable notify
from ISAKMP
```

メイン モード メッセージ 3 (MM3) : NAT 検出および Diffie-Hellman 交換

次が含まれます。

- NAT 検出ペイロードおよびハッシュ
- DH 交換の開始
- Dead Peer Detection （ DPD ）のサポート

```
*Sep 21 08:33:43.437: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel23,
changed state to up
*Sep 21 08:33:43.437: ISAKMP (1011): received packet from 2001: DB8::2 dport
500 sport 500 Global (R) QM_IDLE
*Sep 21 08:33:43.437: ISAKMP: (1011): deleting node 1371333358 error FALSE
reason "QM done (await)"
*Sep 21 08:33:43.437: ISAKMP: (1011):Node 1371333358, Input =
IKE_MESG_FROM_PEER, IKE_QM_EXCH
*Sep 21 08:33:43.437: ISAKMP: (1011): Old State = IKE_QM_R_QM2  New State =
IKE_QM_PHASE2_COMPLETE
*Sep 21 08:33:43.437: IPSEC(key_engine): got a queue event with 1 KMI message(s
*Sep 21 08:33:43.437: IPSEC(key_engine_enable_outbound): rec'd enable notify
from ISAKMP
```

メイン モード メッセージ 4 (MM4) : NAT 検出および Diffie-Hellman 交換

次が含まれます。

- NAT 検出ペイロード
- DH 交換の開始
- 追加の VID (DPD、Unity サポート)
- 別の IOS デバイスとの通信に関する知識

```
*Sep 21 08:33:43.273: ISAKMP (0): received packet from 2001: DB8::3 dport 500
sport 500 Global (I) MM_SA_SETUP
*Sep 21 08:33:43.273: ISAKMP: (0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Sep 21 08:33:43.273: ISAKMP: (0): Old State = IKE_I_MM3  New State = IKE_I_MM4

*Sep 21 08:33:43.273: ISAKMP: (0): processing KE payload. message ID = 0
*Sep 21 08:33:43.281: ISAKMP: (0): processing NONCE payload. message ID = 0
*Sep 21 08:33:43.281: ISAKMP: (0):found peer pre-shared key matching 2001:
DB8::3
*Sep 21 08:33:43.281: ISAKMP: (1011): processing vendor id payload
*Sep 21 08:33:43.281: ISAKMP: (1011): vendor ID is Unity
*Sep 21 08:33:43.281: ISAKMP: (1011): processing vendor id payload
*Sep 21 08:33:43.281: ISAKMP: (1011): vendor ID is DPD
*Sep 21 08:33:43.281: ISAKMP: (1011): processing vendor id payload
*Sep 21 08:33:43.281: ISAKMP: (1011): speaking to another IOS box!
*Sep 21 08:33:43.281: ISAKMP: (1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Sep 21 08:33:43.281: ISAKMP: (1011): Old State = IKE_I_MM4  New State =
IKE_I_MM4
```

メイン モード メッセージ 5 (MM5) : ID の送信

次が含まれます。

- リモート ピア ID (ID)

```
*Sep 21 08:33:43.293: ISAKMP: (1011): Send initial contact
*Sep 21 08:33:43.293: ISAKMP: (1011): SA is doing pre-shared key authentication
using id type ID_IPV6_ADDR
*Sep 21 08:33:43.293: ISAKMP (1011): ID payload
       next-payload : 8
       type         : 5
        address      : 2001: DB8::2
       protocol     : 17
       port         : 500
       length       : 24
*Sep 21 08:33:43.293: ISAKMP: (1011):Total payload length: 24
*Sep 21 08:33:43.293: ISAKMP: (1011): sending packet to 2001: DB8::3 my_port
500 peer_port 500 (I) MM_KEY_EXCH
*Sep 21 08:33:43.293: ISAKMP: (1011): Sending an IKE IPv6 Packet.
*Sep 21 08:33:43.293: ISAKMP: (1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
*Sep 21 08:33:43.293: ISAKMP: (1011): Old State = IKE_I_MM4  New State =
IKE_I_MM5
```

関連コンフィギュレーション：

```
*Sep 21 08:33:43.293: ISAKMP: (1011): Send initial contact
*Sep 21 08:33:43.293: ISAKMP: (1011): SA is doing pre-shared key authentication
using id type ID_IPV6_ADDR
*Sep 21 08:33:43.293: ISAKMP (1011): ID payload
       next-payload : 8
       type         : 5
        address      : 2001: DB8::2
       protocol     : 17
       port         : 500
       length       : 24
*Sep 21 08:33:43.293: ISAKMP: (1011):Total payload length: 24
*Sep 21 08:33:43.293: ISAKMP: (1011): sending packet to 2001: DB8::3 my_port
500 peer_port 500 (I) MM_KEY_EXCH
*Sep 21 08:33:43.293: ISAKMP: (1011): Sending an IKE IPv6 Packet.
*Sep 21 08:33:43.293: ISAKMP: (1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
*Sep 21 08:33:43.293: ISAKMP: (1011): Old State = IKE_I_MM4  New State =
IKE_I_MM5
```

メイン モード メッセージ 6 (MM6) ：リモート ピア ID、フェーズ 1 が確立されます。

次が含まれます。

- キー再生成時刻が開始します。
- リモート ID (この場合はアドレス)
- プロファイルで受信する決定

```
*Sep 21 08:33:43.297: ISAKMP (1011): received packet from 2001: DB8::3 dport
500 sport 500 Global (I) MM_KEY_EXCH
*Sep 21 08:33:43.297: ISAKMP: (1011): processing ID payload. message ID = 0
*Sep 21 08:33:43.297: ISAKMP (1011): ID payload
       next-payload : 8
       type         : 5
       address      : 2001: DB8::3
       protocol     : 17
       port         : 500
```

```
       length       : 24
*Sep 21 08:33:43.297: ISAKMP: (0):: peer matches *none* of the profiles
*Sep 21 08:33:43.297: ISAKMP: (1011): processing HASH payload. message ID = 0
*Sep 21 08:33:43.297: ISAKMP: (1011): SA authentication status: authenticated
*Sep 21 08:33:43.297: ISAKMP: (1011): SA has been authenticated with 2001:
DB8::3
*Sep 21 08:33:43.297: ISAKMP: Trying to insert a peer 2001: DB8::2/2001:
DB8::3/500/,  and inserted successfully 9344BE8.
*Sep 21 08:33:43.297: ISAKMP: (1011):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Sep 21 08:33:43.297: ISAKMP: (1011): Old State = IKE_I_MM5  New State =
IKE_I_MM6

*Sep 21 08:33:43.297: ISAKMP: (1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Sep 21 08:33:43.297: ISAKMP: (1011): Old State = IKE_I_MM6  New State =
IKE_I_MM6

*Sep 21 08:33:43.301: ISAKMP: (1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
*Sep 21 08:33:43.301: ISAKMP: (1011): Old State = IKE_I_MM6  New State =
IKE_P1_COMPLETE
```

関連コンフィギュレーション：

```
*Sep 21 08:33:43.297: ISAKMP (1011): received packet from 2001: DB8::3 dport
500 sport 500 Global (I) MM_KEY_EXCH
*Sep 21 08:33:43.297: ISAKMP: (1011): processing ID payload. message ID = 0
*Sep 21 08:33:43.297: ISAKMP (1011): ID payload
       next-payload : 8
       type         : 5
       address      : 2001: DB8::3
       protocol     : 17
       port         : 500
       length       : 24
*Sep 21 08:33:43.297: ISAKMP: (0):: peer matches *none* of the profiles
*Sep 21 08:33:43.297: ISAKMP: (1011): processing HASH payload. message ID = 0
*Sep 21 08:33:43.297: ISAKMP: (1011): SA authentication status: authenticated
*Sep 21 08:33:43.297: ISAKMP: (1011): SA has been authenticated with 2001:
DB8::3
*Sep 21 08:33:43.297: ISAKMP: Trying to insert a peer 2001: DB8::2/2001:
DB8::3/500/,  and inserted successfully 9344BE8.
*Sep 21 08:33:43.297: ISAKMP: (1011):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Sep 21 08:33:43.297: ISAKMP: (1011): Old State = IKE_I_MM5  New State =
IKE_I_MM6

*Sep 21 08:33:43.297: ISAKMP: (1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Sep 21 08:33:43.297: ISAKMP: (1011): Old State = IKE_I_MM6  New State =
IKE_I_MM6

*Sep 21 08:33:43.301: ISAKMP: (1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
*Sep 21 08:33:43.301: ISAKMP: (1011): Old State = IKE_I_MM6  New State =
IKE_P1_COMPLETE
```

クイック モード メッセージ 1（QM1）：ピアがフェーズ 2 を開始します。

次が含まれます。

- リモートおよびローカル プロキシ ID
- トランスフォーム セット

```
*Sep 21 08:33:43.297: ISAKMP (1011): received packet from 2001: DB8::3 dport
500 sport 500 Global (I) MM_KEY_EXCH
*Sep 21 08:33:43.297: ISAKMP: (1011): processing ID payload. message ID = 0
*Sep 21 08:33:43.297: ISAKMP (1011): ID payload
       next-payload : 8
       type         : 5
       address      : 2001: DB8::3
       protocol     : 17
       port         : 500
       length       : 24
*Sep 21 08:33:43.297: ISAKMP: (0):: peer matches *none* of the profiles
*Sep 21 08:33:43.297: ISAKMP: (1011): processing HASH payload. message ID = 0
*Sep 21 08:33:43.297: ISAKMP: (1011): SA authentication status: authenticated
*Sep 21 08:33:43.297: ISAKMP: (1011): SA has been authenticated with 2001:
DB8::3
*Sep 21 08:33:43.297: ISAKMP: Trying to insert a peer 2001: DB8::2/2001:
DB8::3/500/,  and inserted successfully 9344BE8.
*Sep 21 08:33:43.297: ISAKMP: (1011):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Sep 21 08:33:43.297: ISAKMP: (1011): Old State = IKE_I_MM5  New State =
IKE_I_MM6

*Sep 21 08:33:43.297: ISAKMP: (1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Sep 21 08:33:43.297: ISAKMP: (1011): Old State = IKE_I_MM6  New State =
IKE_I_MM6

*Sep 21 08:33:43.301: ISAKMP: (1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
*Sep 21 08:33:43.301: ISAKMP: (1011): Old State = IKE_I_MM6  New State =
IKE_P1_COMPLETE
```

関連コンフィギュレーション：

```
*Sep 21 08:33:43.297: ISAKMP (1011): received packet from 2001: DB8::3 dport
500 sport 500 Global (I) MM_KEY_EXCH
*Sep 21 08:33:43.297: ISAKMP: (1011): processing ID payload. message ID = 0
*Sep 21 08:33:43.297: ISAKMP (1011): ID payload
       next-payload : 8
       type         : 5
       address      : 2001: DB8::3
       protocol     : 17
       port         : 500
       length       : 24
*Sep 21 08:33:43.297: ISAKMP: (0):: peer matches *none* of the profiles
*Sep 21 08:33:43.297: ISAKMP: (1011): processing HASH payload. message ID = 0
*Sep 21 08:33:43.297: ISAKMP: (1011): SA authentication status: authenticated
*Sep 21 08:33:43.297: ISAKMP: (1011): SA has been authenticated with 2001:
DB8::3
*Sep 21 08:33:43.297: ISAKMP: Trying to insert a peer 2001: DB8::2/2001:
DB8::3/500/,  and inserted successfully 9344BE8.
*Sep 21 08:33:43.297: ISAKMP: (1011):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Sep 21 08:33:43.297: ISAKMP: (1011): Old State = IKE_I_MM5  New State =
IKE_I_MM6

*Sep 21 08:33:43.297: ISAKMP: (1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Sep 21 08:33:43.297: ISAKMP: (1011): Old State = IKE_I_MM6  New State =
IKE_I_MM6

*Sep 21 08:33:43.301: ISAKMP: (1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
*Sep 21 08:33:43.301: ISAKMP: (1011): Old State = IKE_I_MM6  New State =
IKE_P1_COMPLETE
```

クイック モード メッセージ 2 (QM2)

次が含まれます。

- プロキシ ID の確認
- トンネル タイプ
- Perfect Forwarding Secrecy (PFS) 設定

```
*Sep 21 08:33:43.297: ISAKMP (1011): received packet from 2001: DB8::3 dport
500 sport 500 Global (I) MM_KEY_EXCH
*Sep 21 08:33:43.297: ISAKMP: (1011): processing ID payload. message ID = 0
*Sep 21 08:33:43.297: ISAKMP (1011): ID payload
       next-payload : 8
       type         : 5
       address      : 2001: DB8::3
       protocol     : 17
       port         : 500
       length       : 24
*Sep 21 08:33:43.297: ISAKMP: (0):: peer matches *none* of the profiles
*Sep 21 08:33:43.297: ISAKMP: (1011): processing HASH payload. message ID = 0
*Sep 21 08:33:43.297: ISAKMP: (1011): SA authentication status: authenticated
*Sep 21 08:33:43.297: ISAKMP: (1011): SA has been authenticated with 2001:
DB8::3
*Sep 21 08:33:43.297: ISAKMP: Trying to insert a peer 2001: DB8::2/2001:
DB8::3/500/,  and inserted successfully 9344BE8.
*Sep 21 08:33:43.297: ISAKMP: (1011):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Sep 21 08:33:43.297: ISAKMP: (1011): Old State = IKE_I_MM5  New State =
IKE_I_MM6

*Sep 21 08:33:43.297: ISAKMP: (1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Sep 21 08:33:43.297: ISAKMP: (1011): Old State = IKE_I_MM6  New State =
IKE_I_MM6

*Sep 21 08:33:43.301: ISAKMP: (1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
*Sep 21 08:33:43.301: ISAKMP: (1011): Old State = IKE_I_MM6  New State =
IKE_P1_COMPLETE
```

関連コンフィギュレーション：

```
*Sep 21 08:33:43.297: ISAKMP (1011): received packet from 2001: DB8::3 dport
500 sport 500 Global (I) MM_KEY_EXCH
*Sep 21 08:33:43.297: ISAKMP: (1011): processing ID payload. message ID = 0
*Sep 21 08:33:43.297: ISAKMP (1011): ID payload
       next-payload : 8
       type         : 5
       address      : 2001: DB8::3
       protocol     : 17
       port         : 500
       length       : 24
*Sep 21 08:33:43.297: ISAKMP: (0):: peer matches *none* of the profiles
*Sep 21 08:33:43.297: ISAKMP: (1011): processing HASH payload. message ID = 0
*Sep 21 08:33:43.297: ISAKMP: (1011): SA authentication status: authenticated
*Sep 21 08:33:43.297: ISAKMP: (1011): SA has been authenticated with 2001:
DB8::3
*Sep 21 08:33:43.297: ISAKMP: Trying to insert a peer 2001: DB8::2/2001:
DB8::3/500/,  and inserted successfully 9344BE8.
*Sep 21 08:33:43.297: ISAKMP: (1011):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Sep 21 08:33:43.297: ISAKMP: (1011): Old State = IKE_I_MM5  New State =
IKE_I_MM6
```

```
*Sep 21 08:33:43.297: ISAKMP: (1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Sep 21 08:33:43.297: ISAKMP: (1011): Old State = IKE_I_MM6  New State =
IKE_I_MM6

*Sep 21 08:33:43.301: ISAKMP: (1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
*Sep 21 08:33:43.301: ISAKMP: (1011): Old State = IKE_I_MM6  New State =
IKE_P1_COMPLETE
```

クイック モード メッセージ 3 (QM3) : フェーズ 2 の確立

次が含まれます。

- トラフィックを渡すセキュリティ ポリシー インデックス (SPI) の設定

```
*Sep 21 08:33:43.305: ISAKMP: (1011): Sending an IKE IPv6 Packet.
*Sep 21 08:33:43.305: ISAKMP: (1011): deleting node 1371333358 error FALSE
reason "No Error"
*Sep 21 08:33:43.305: ISAKMP: (1011):Node 1371333358, Input =
IKE_MESG_FROM_PEER, IKE_QM_EXCH
*Sep 21 08:33:43.305: ISAKMP: (1011): Old State = IKE_QM_I_QM1  New State =
IKE_QM_PHASE2_COMPLETE
*Sep 21 08:33:43.305: IPSEC(key_engine): got a queue event with 1 KMI message(s)
*Sep 21 08:33:43.305: IPSEC(crypto_ipsec_create_ipsec_sas): Map found
Tunnel23-head-0
*Sep 21 08:33:43.305: IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting
with the same proxies and peer 2001: DB8::3
*Sep 21 08:33:43.305: IPSEC(create_sa): sa created,
 (sa) sa_dest= 2001: DB8::2, sa_proto= 50,
   sa_spi= 0x45F16A9A(1173449370),
   sa_trans= esp-aes esp-sha-hmac , sa_conn_id= 305
   sa_lifetime(k/sec)= (4608000/3439)
*Sep 21 08:33:43.305: IPSEC(create_sa): sa created,
 (sa) sa_dest= 2001: DB8::3, sa_proto= 50,
   sa_spi= 0x221A7153(572158291),
   sa_trans= esp-aes esp-sha-hmac , sa_conn_id= 306
   sa_lifetime(k/sec)= (4608000/3439)
R2(config-if)#
*Sep 21 08:33:43.309: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Tunnel23, changed state to up
```

トンネルの確認

```
sh crypto ipsec sa

interface: Tunnel23
   Crypto map tag: Tunnel23-head-0, local addr 2001: DB8::2

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (::/0/0/0)
  remote ident (addr/mask/prot/port): (::/0/0/0)
  current_peer 2001: DB8::3 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0
```

```
    local crypto endpt.: 2001: DB8::2,
    remote crypto endpt.: 2001: DB8::3
    path mtu 1500, ipv6 mtu 1500, ipv6 mtu idb Ethernet0/0
    current outbound spi: 0x221A7153(572158291)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
      spi: 0x45F16A9A(1173449370)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 305, flow_id: SW:305, sibling_flags 80000041, crypto map:
Tunnel23-head-0
       sa timing: remaining key lifetime (k/sec): (4183789/3408)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
      spi: 0x221A7153(572158291)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 306, flow_id: SW:306, sibling_flags 80000041, crypto map:
Tunnel23-head-0
       sa timing: remaining key lifetime (k/sec): (4183790/3408)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE

R2(config-if)#do ping fe80::23:3
Output Interface: tunnel23
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FE80::23:3, timeout is 2 seconds:
Packet sent with a source address of FE80::23:2%Tunnel23
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/11/20 ms
R2(config-if)#do sh crypto ipsec sa | i caps|ident
  local  ident (addr/mask/prot/port): (::/0/0/0)
  remote ident (addr/mask/prot/port): (::/0/0/0)
    #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
    #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
```

トンネルはアップしており、トラフィックを渡しています。

関連情報

- IPSec に関する Wikipedia の記事 ： 標準および参考文献には多くの有用な情報が含まれています。
- ASA IPsec および IKE デバッグ (IKEv1 アグレッシブ モード) のトラブルシューティングに関するテクニカル ノート
- ASA IPsec および IKE のデバッグ (IKEv1 メイン モード) のトラブルシューティング テクニカルノート
- テクニカルサポートとドキュメント - Cisco Systems